

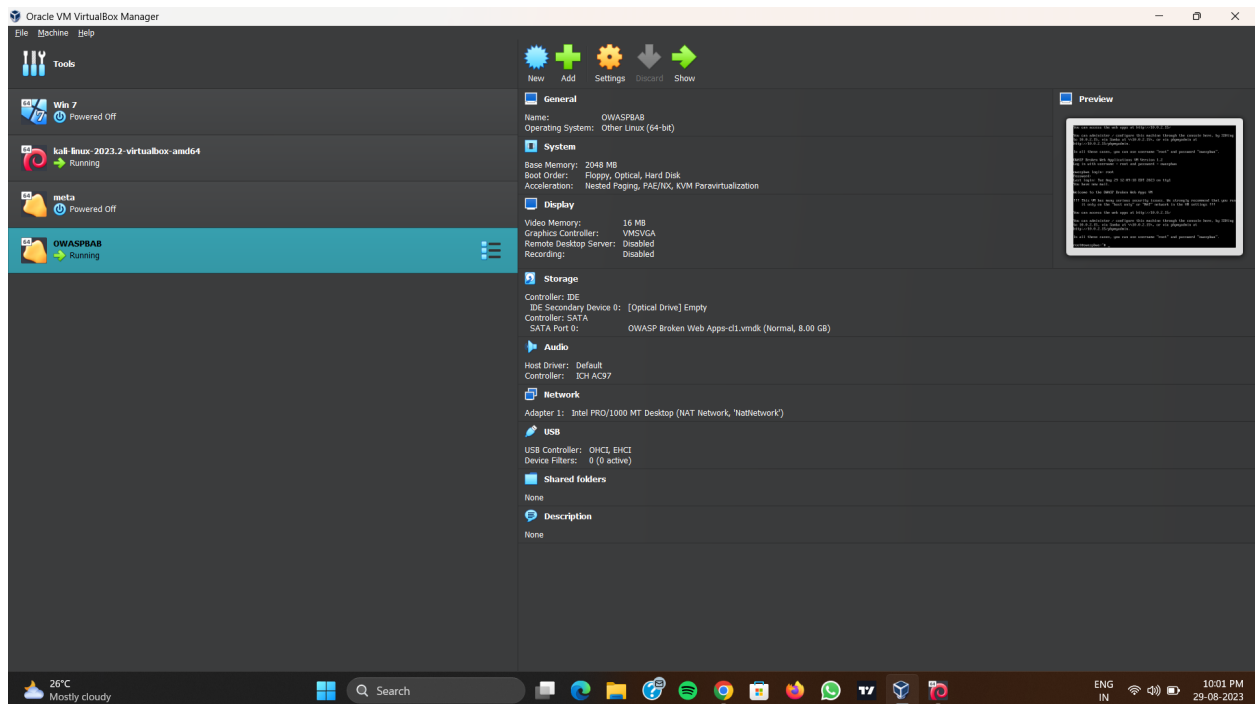
# CROSS SITE SCRIPTING (XSS)

OWASP stands for Open worldwide Application security project. It is usually used for web application testing.

## Steps to start OWASP.

- 1.Start OWASP on virtual machine.
- 2.Enter the credentials and login.
- 3.Open firefox and enter the OWASP ip address.
- 4.Select the web application you want.

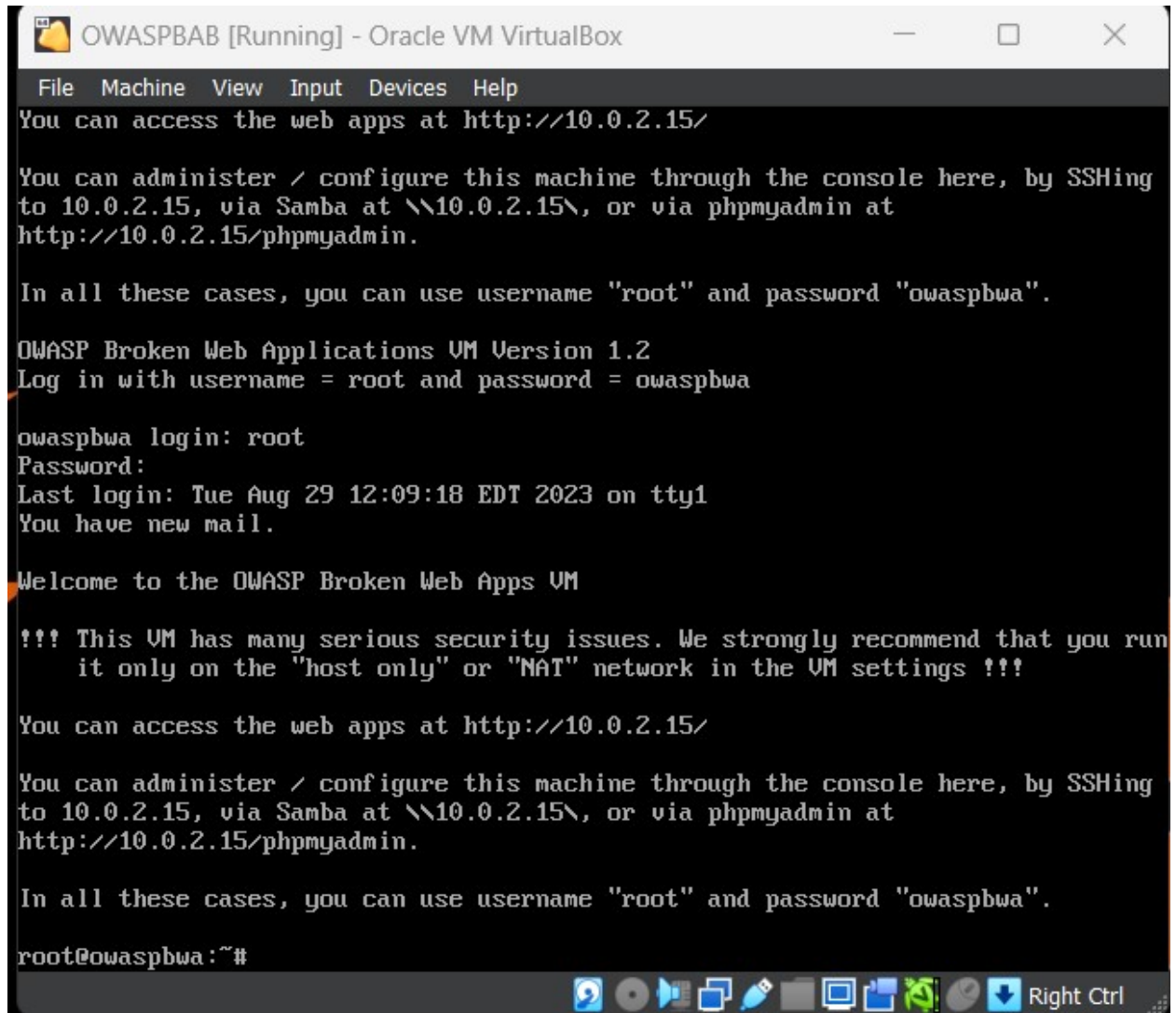
## 1.Start the OWASP on virtual machine.



It will take some time and opens up prompt. Wait for it to fully load and then enter the login id and password.

## 2.Entering the credentials and login.

The login credentials are root and password is owaspbwa.



```
OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Last login: Tue Aug 29 12:09:18 EDT 2023 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.0.2.15/

You can administer / configure this machine through the console here, by SSHing
to 10.0.2.15, via Samba at \\10.0.2.15\\, or via phpmyadmin at
http://10.0.2.15/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~#
```

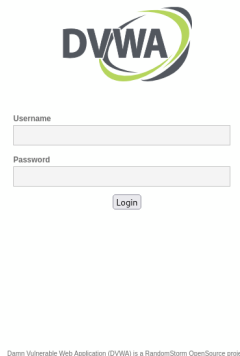
Now we can any browser and type the owasp ip address as shown in the prompt. Note that if both kali and owasp are in the NAT network then only the result will come. Otherwise it will not come. You can change it in settings of owasp.

### 3.Open firefox and enter the ip address

Open the firefox or any other browser and type the ip address of the owasp.



On entering the address it will show above page. Here the select the application as per your need. But here we need to select Damn Vulnerable Web Application.



On clicking it, a new page will open like above. Enter the username and password as admin and admin. It will lead to a new page where the contents looks like below.

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Username: admin  
Security Level: low  
PHPIDS: disabled

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Damn Vulnerable Web Application (DVWA) v1.8

Here select the xss reflected. XSS means cross-site scripting. That is, here we can modify the html, javascript of a website . On clicking the XSS reflected option page like below will be opened.



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected**
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

Here in what's your name section, enter your name.

Upon clicking submit the below is shown.

**DVWA**

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello shrinivas

### More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>


Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.8

The name field we can enter the html code as `<h1> YOUR NAME</h1>`

And the result will be like the following image. This means that the name field is not only taking the input but is also executing it. We can also add javascript to it.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?  
  
Hello  
**ABC**

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

View Source

View Help

Username: admin

Security Level: low

PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Damn Vulnerable Web Ap x

10.0.2.15/dvwa/vulnerabilities/xss\_r?name=<script>alert('Hi!+how+is+y

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?  
  
Hello

10.0.2.15

Hi ! how is your day today

OK

Read 10.0.2.15